數學傳播　48卷3期, pp. 20-23

橢圓曲線上的代數、幾何以及應用

陳榮凱

橢圓曲線是數學當中相當有趣的題材, 在數學中的一些重要領域, 例如代數、幾何、分析、數論等等面向都可以發現它的身影, 本文計畫從各個面向介紹橢圓曲線以及在密碼學上的應用。

一、平面上的曲線

代數幾何所討論的對象主要是代數多樣體, 所謂的代數多樣體簡單來說考慮的就是一個在射影空間 (projective space) 或者是仿射空間 (affine space) 中由多項式所定義的幾何物件。例如 $y-x^2$ 這樣的二元二次多項式定義了平面上的一條二次曲線, 因此可以視爲仿射平面上的代數多樣體, 若是將此拋物線補上無窮遠點則形成射影平面上的代數多樣體 C, 補上無窮遠點的動作可以藉由將 $y-x^2$ 齊次化成爲 $YZ-X^2$ 來實現。

在射影幾何中的一個基本定理是 Bezout's Theorem:

定理 1: 在複數射影平面上, 沒有公因式的 m 次曲線和 n 次曲線, 交點重數的和恰爲 mn。

簡單來說, 在通常沒有重根的情況下會恰有 mn 個交點。以剛才拋物線 C 的例子來看, C 可以視爲二次曲線。考慮 $a>0$ 的實數, 和 $y=a$ 這樣的直線 (一次曲線) 交於兩實數點; 若考慮 $a<0$ 的實數, 和 $y=a$ 這樣的直線則交於兩複數點; 若再考慮和 $y=0$ 這樣的直線則交於一點具有交點重數爲 2。此外, 若是考慮 $x=a$, 則會有一個交點在平面上, 以及另一個在 $(0,1)$ 方向無窮遠點的交點。

二、三次曲線上的代數

我們接著考慮平面上由 $y^2=x(x-1)(x-\lambda)$ 所定義的三次曲線 C, 其中 λ 是一個不等於 0 或是 1 的數, 補上在 (0,1) 方向無窮遠點 o, 則得到射影平面中由 $Y^2Z=X(X-Z)(X-\lambda Z)$ 所定義的三次曲線 E, 在這三次曲線 E 上有著非常特殊的代數結構。

首先注意的是一般的直線 L 與此三次曲線 E 會有三個交點 P、Q、R。換句話說, 任意給三次曲線 E 上面的兩點 P 和 Q, 透過 P 和 Q 的連線 L 可以決定出唯一的第三點 R, 也可以

說 P 和 Q「運算」後得到 R。考慮 $P*Q$ 爲 R 的對稱點, 這樣修正後的運算有以下的結果:

定理 2: 三次曲線 E 上有一個群的運算 $*$, 使得 o 爲運算 $*$ 的單位元素; $P=(a,b)$ 的反元素爲 $-P=(a,-b)$; 直線 L 與此三次曲線 E 的三個交點 P、Q、R 滿足 $P*Q*R=o$。

簡單來說, 三次曲線 E 搭配運算 $*$ 形成一個交換群。給定這樣代數運算的三次曲線 E 我們稱之爲橢圓曲線。

三、橢圓曲線上的算術

在上述所考慮的橢圓曲線中, 如果我們選取 λ 是一個有理數, 則任何兩有理點 P 和 Q 運算後得到 $P*Q$ 也會是有理點。舉例來說, 在橢圓曲線上考慮有理點 $P=(a,b)$, $Q=(c,d)$, 其中 a,b,c,d 均爲有理數, PQ 的連線 L 的方程式可以寫成 $y=mx+n$, 其中 m、n 都是有理數。令 $R=(e,f)$ 是 L 交 E 所得到的第三點, 我們可以算出 $a+c+e=(\lambda+1+m^2)$, 所以 e 也是有理數, 另外 $f=me+n$ 也是有理數, 這也保證 $P*Q=(e,-f)$ 是個有理點。收集所有的有理點, 記爲 $E(\mathbb{Q})$, 則 $E(\mathbb{Q})$ 形成橢圓曲線 E 的一個子群。

相當知名的 Mordell-Weil 定理告訴我們 $E(\mathbb{Q})$ 事實上是一個有限生成的交換群; 有限生成交換群的基本定理保證任何有限生成的交換群可以分解成 $\mathbb{Z}^r$ 和 T 兩部分, 其中 T 是有限群, r 是非負整數, 定義爲橢圓曲線的 rank, 這是橢圓曲線上一個基本的不變量。許多數論上的問題往往可以透過對於橢圓曲線的研究來呈現並進而解決。

四、複數函數的因子

我們先前透過三次曲線上的運算看到代數結構而得到橢圓曲線, 以下我們試圖在複數平面的商群上描繪出三次曲線的樣貌。首先, 在複數平面上複數可微分的函數我們稱之爲全純函數 (holomorphic function), 在極點 (pole) 以外皆可微分的函數我們稱之爲亞純函數 (meromorphic function)。標準的亞純函數例子像是形如 $f(z)=(z-1)^4/(z-2)^2$ 的有理函數, 它在 $z=1$ 這一點是一個 4 階 (order 4) 的零點 (zero), 在 $z=2$ 這一點是一個 2 階 (order 2) 的極點 (pole)。事實上, 若是在複數平面補上一個無窮遠點 ∞, 則會形成黎曼球面 (Riemann sphere); 我們用 S 來表示此黎曼球面, 則原來在複數平面上的亞純函數就可以理解成從 S 到 S 的全純映射。在無窮遠點 ∞ 附近我們可以用 $w=1/z$ 的代換來討論, 當 $w=0$ 時就對應到 $z=\infty$。像剛才 $f(z)=(z-1)^4/(z-2)^2$ 的例子, 經由 $w=1/z$ 的代換會得到 $f=(1-w)^4/w^2(1-2w)^2$, 這時我們看到的零點和極點: 除了原本 $z=1$ (也就是 $w=1$) 以及在 $z=2$ (也就是 $w=1/2$) 以外, 我們額外看到 $w=0$ (也就是 $z=\infty$) 這一個 2 階的極點。

在以上的討論中, 零點和極點以及它們的階數可謂是最重要的訊息, 我們可以引進複數函數的因子 (divisor) 這樣的概念來描述零點和極點以及它們的階數, 像是 f 的因子我們可以寫成 $4[z=1]-2[z=2]-2[z=\infty]$ 這樣的因子。可以注意到這個因子係數和爲 $4-2-2=0$。

透過留數定理 (Residue Theorem) 的技巧, 運用在類似於黎曼球面的緊緻黎曼曲面 (compact Riemann surface) 上, 可以證明亞純函數產生的因子都具有係數和爲 0 的現象。有名的 Riemann-Roch Theorem, 則是用來推估緊緻黎曼曲面上滿足特定因子條件的亞純函數空間之維度。一般來說, 極點越多或是階數越大則越容易找到滿足條件的亞純函數。

五、橢圓曲線上的因子

複數平面 $\mathbb{C}$ 上, 搭配加法運算形成一個交換群。我們再考慮由整數格子點 $a+bi$ (其中 a,b 爲整數) 所形成的加法子群 Λ, 這樣所產生的商群 (quotient group) $W := \mathsf{C}/\Lambda$ 也還是個交換群。注意到商群的意義即是將相差 $a+bi$ 的點視爲同一組, 所以定義在 W 上的函數恰對應到複數平面上滿足 $f(z+a+bi)=f(z)$ 的函數, 也就是滿足 $f(z+1)=f(z)$, $f(z+i)=f(z)$ 的雙周期函數。這樣的雙周期函數的函數值, 其實可以完全由函數在基本域 (fundamental domain) $D:=\{c+di \mid 0\le c,d<1\}$ 的函數值來決定。

透過複變函數論的一些標準定理可以證明雙周期全純函數必爲常數函數。透過留數定理也可以發現: 即使是允許有階數爲 1 的單極點的亞純雙周期函數也只能是常數函數。最基本的亞純雙周期函數是 Weierstrass P-function $\wp(z)$. 這個函數在基本域上只有一個階數爲 2 的極點。如果繼續往下看, P-function 的微分 $\wp'(z)$ 有一個階數爲 3 的極點, $\wp(z)^3$ 和 $\wp'(z)^2$ 都有階數爲 6 的極點, 事實上, 兩者之間有以下的關係

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

這也告訴我們如果考慮 $\Phi: W \to \mathbb{C}^2$, 將 $z \mapsto (\wp(z), \wp'(z))$, 則 $\Phi(W)$ 在 $\mathbb{C}^2$ 中滿足 $y^2=4x^3-g_2x-g_3$, 換句話說, $\Phi(W)$ 落在由 $y^2=4x^3-g_2x-g_3$ 所定義的三次曲線上。注意到 Φ 函數在 $z=0$ 這點是沒有定義的, 事實上, 若是將 $\Phi(0)$ 定爲 $(0,1)$ 方向的無窮遠點 o, 則會發現 $\Phi: W\to\mathbb{P}^2$ 給出了一個 W 到射影平面三次曲線 $Y^2Z=4X^3-g_2XZ^2-g_3Z^3$ 的一對一對應, 所以 W 這樣的一個商群 (也是一個緊緻黎曼曲面) 也可以視爲一個三次曲線。更進一步可以發現該映射其實是一個群同構 (group isomorphism)。

六、橢圓曲線在密碼學上的應用

最後我們討論橢圓曲線在密碼學上的應用。給橢圓曲線 E 上一點 P, 決定 $2P=P*P$ 的方式可以透過 P 點的切線所交出來的第三點來決定。反之, 如果給定 Q 且已知 $Q=2P$, 可以利用上述的算法求出 P。但是如果給定 Q 且已知 $Q=mP$, 當 m 很大時, 求出 P 就變成非

常困難的問題。從上述的原理出發, 考慮在有限體上的橢圓曲線, 給定 P, Q 且已知 $Q = mP$ 而試圖求出 m 就是所謂的 Discrete logarithm problem (DLP) 也是非常困難的問題。橢圓曲線密碼學 (Elliptic curve cryptography) 即是利用有限體上橢圓曲線的 DLP 所設計的一個系統, 是目前相當被廣泛使用的一套系統。

結語

以上的討論說明了橢圓曲線的許多面向: 定義在複數時, 它同時可以視為射影平面中的三次曲線, 也同時是一個緊緻的黎曼曲面; 定義在有理數或是有限體時, 又會有許多有趣的算術性質。透過不同的觀點, 以及彼此間的聯繫, 讓我們對於橢圓曲線的本質有更多的認識。雖然我們通常學習數學時, 往往是分成代數、分析、幾何等分主題的學習, 但是不同領域其實是彼此交織在一起的, 保持著開放的心, 欣賞不同角度所帶來的不同的景象, 可以看到另一番景象。

—本文作者任教於台灣大學數學系—